

REMARKS

Claims 1-22 are pending in this application. Claims 1-8, 12-22 were rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 5,499,294 to Friedman ("Friedman") in view of U.S. Patent No. 5,875,249 to Mintzer et al. ("Mintzer"). Claim 9 was rejected under 35 U.S.C. §103(a) as being unpatentable over Friedman in view of Mintzer in further view of U.S. Patent No. 5,799,082 to Murphy et al. ("Murphy"). Claims 10-11 were rejected under 35 U.S.C. §103(a) as being unpatentable over Friedman in view of Mintzer and in further view of U.S. Patent No. 5,335,072 to Tanaka et al ("Tanaka"). Applicants respectfully traverse the rejections.

To establish a *prima facie* case of obviousness against claim 1, at the very least, the combination of Friedman and Mintzer must teach or suggest all the claim elements. Here, the combination of Friedman and Mintzer is legally deficient because, *at the very minimum*, the combination does not teach or suggest (i) an information receiving means for receiving data associated with a user when the digital image is generated, (ii) a wireless communication means for receiving data from an object in an observed image frame when the image is generated or (iii) image processing means for recording the received user data and object data in a captured image, as essentially claimed in claim 1.

Examiner contends that the "digital code" or private key described in Col. 3, lines 1-11, of Friedman discloses the "information receiving means" for receiving user data, as essentially claimed in claim 1. It is respectfully submitted that this interpretation is erroneous. Friedman discloses in Col. 2, line 60 through Col. 3, line 11, nothing more than a well-known method for processing a digital signature. As explained in the cited section, a digital signature is generated by hashing a message using an algorithm and encrypting the message using a private key. A

public key is then used to decrypt the hashed message. The authenticity of a message is determined by decrypting the digital signature with the public key and comparing the decrypted digital signature with a hash of the message in question to determine if they are the same. Friedman discloses a method for authenticating digital image files using digital signatures. Friedman teaches that a digital camera comprises means for encrypting a hash of the image file using a private key that is not known by anyone except the manufacturer of the camera system or the encrypting means implemented, and that the user only knows the public key for decrypting a digital signature of an image file (see, e.g., Col. 4, lines 30-46).

Therefore, Examiner's contention that Friedman teaches a "digital code" for associating data with a user of the system" and that "the transmission of a digital signature can only be associated with the private key holder" has absolutely no relation to, and is nothing more than a strained interpretation of, the claimed feature of information "receiving means" for receiving data associated with the user of the system when the image is generated. Indeed, the "private key" is associated with the camera and not the user of the camera, as incorrectly contended. Further, the private key is not "received" from a user *via* an information receiving means, but the private key is rather embedded in, and made part of, the camera processor. Further, the private key simply does not constitute user data that is recorded in an image file.

Next, it is respectfully submitted that Examiner's interpretation of the "range finding" means of Friedman as disclosing a "wireless communication means ... for receiving data from objects" is erroneous. The term "communication" implies that there is an exchange of some data between the image capturing system and object in the scene. With range finding as disclosed by Friedman, acoustic or infrared signals are first transmitted by the system and then the reflected signals from an object are captured by the system, wherein the total time of travel of

the transmitted and reflected signals is used to determine the range. Thus, there is no "wireless communication" of object data *per se* with such range finding techniques.

Thus, for at least the reasons given above, combination of Friedman and Mintzer is legally deficient to sustain a rejection of claim 1 under 35 U.S.C. 103(a). Further, claims 2-8 and 12 depend from claim 1 and are, thus, believed to be patentable over the combination of Friedman and Mintzer for at least the reasons given above for claim 1.

In addition, since claims 9, 10 and 11 depend from claim 1, the rejection of claim 9 under 35 U.S.C. §103(a) over the combination of Friedman, Mintzer and Murphy, as well as the rejection of claims 10-11 under 35 U.S.C. §103(a) over the combination of Friedman, Mintzer and Tanaka, is legally deficient for at least the reasons given above for claim 1. Indeed, the rejection of such claims is based, in part, on the contention that Friedman and Mintzer disclose all the elements of claim 1 which, as demonstrated above, is erroneous. Further, neither Murphy nor Tanaka cures the deficiencies of Friedman and Mintzer in that neither Murphy nor Tanaka discloses or suggests, for example, information receiving means for receiving data associated with a user of said system when said digital image is generated, much less a wireless communication means for receiving data from objects in an observed image frame when the image is generated, as essentially claimed in claim 1.

Next, with respect to the rejection of claims 13 and 18 under 35 U.S.C. §103(a) as being unpatentable over Friedman and Mintzer, it is respectfully submitted that the combination of Friedman and Mintzer is legally deficient because, the combination of Friedman and Mintzer does not disclose a method for watermarking a plurality of recorded parameters in an image. Indeed, as acknowledged in the Office Action, Friedman does not disclose means for watermarking a plurality of parameters into the image. Furthermore, although Mintzer discloses

watermarking, Mintzer expressly discloses watermarking trademarks and graphic symbols, but does not expressly disclose watermarking recorded camera parameters.

Furthermore, with respect to claim 18 (as well as claims 2 and 3), given the acknowledgement on page 7, paragraph 1, of the Office Action that neither Friedman nor Mintzer explicitly discloses means for specifying or determining which of the plurality of parameters should be recorded or watermarked in the image, it is respectfully submitted that the conclusion that such claimed element is obvious is nothing more than impermissible hindsight.

Thus, for at least the above reasons, claims 13 and 18 are believed to be patentable over the combination of Friedman and Mintzer.

Claims 14-17 and 21 depend from claim 13 and are believed to be allowable at least by virtue of their dependence from claim 13. Claims 19-20 and 22 depend from claim 18 and are believed to be allowable at least by virtue of their dependence from claim 18.

Accordingly, for at least all of the above reasons, the withdrawal of the rejections of claims 1-22 under §103 is respectfully requested.

Early and favorable consideration of this application is earnestly solicited.

Respectfully submitted,



Frank V. DeRosa
Reg. No. 43,584
Attorney for Applicant(s)

F. Chau & Associates, LLP
1900 Hempstead Turnpike
Suite 501
East Meadow, NY 11554
TEL.: (516) 357-0091
FAX: (516) 357-0092